

NELSON March 67

A REPORT FOR BUSINESS ON THE
USES AND ABUSES OF INDUSTRIAL SECURITY EQUIPMENT

A White Paper Prepared By:

Zelex Marketing Corporation

866 United Nations Plaza

New York City, N. Y.

(212) 421-1666

For: _____

TABLE OF CONTENTS

Introduction	Page 1
Putting Industrial Security To Work For Business	Page 3
The Many Meaningful Business Applications of Electronic Listening Devices	Page 6
An Ounce Of Prevention	Page 9
Cost Analysis Chart	Page 10
Protecting Against Industrial Espionage	Page 14

INTRODUCTION

By the time you read this booklet it may be obsolete.

We live in an age where today's miraculous electronic achievement is tomorrow's antique. This is particularly true in the field of industrial security.

The miniature microphone in the martini olive that caused such a stir not so long ago is as outmoded today as the steam engine. And devices such as sugar cube size transmitters that today are considered the ultimate in sophisticated electronic engineering, will, within a short time, undoubtedly be looked upon as crude and antiquated.

Therefore, this booklet is not intended to be a definitive catalogue of electronic envesdropping and anti-snooping devices, but a report on the ways in which management is and can utilize these new fact finding tools. With information the lifeblood of so many businesses and industries, the lengths to which firms will go to secure the secrets of their competitors while guarding their own plans, ideas and processes has gone far beyond anything the business world has ever before witnessed.

Whether you have or will ever find use for this new breed of industrial security device, as a businessman you should be aware of their existence, their potential, the danger they represent when used by the wrong people, and any possible applications they might have insofar as your organization is concerned. That is the purpose of this booklet - - - - to clearly outline the concept, uses

-more-

and abuses of a growing group of specialized electronic apparatus that is changing management practices and approaches throughout the world.

Unfortunately, we live in a society where "do unto your competitor before he does it unto you" is more often the rule than the exception. When you read the material in this booklet, bear in mind the possibility exists that if you don't take the information and advice contained in this report to heart, your competitor may.

SECTION I

PUTTING INDUSTRIAL SECURITY
TO WORK FOR BUSINESS

When the Atom Bomb was first perfected, a noted scientist made the observation that now there was no place to hide.

The same comment could be made today about electronic eaves-dropping devices. In a parallel sense, the long range effect on a business that ignores the implications of these newest technological advances can end up being as devastating as the dropping of the A Bomb was on Hiroshima.

Since most firms will camouflage their expenditures on electronic surveillance equipment under a variety of different headings, it is impossible to accurately ascertain exactly how much business and industry spends in this area. However, there are a few sign posts that give an indication of what value many companies place on these new devices.

Recently, one of the world's largest food producers revealed it had allocated a million-and-a-quarter dollars for "internal security". The company was not referring to night watchmen.

Millions, perhaps even billions, of dollars are being spent annually by American business to protect itself both from within and without.

-more-

The question that arises is - - is this panic or a practical evaluation of the needs of business in our modern society? The best answer that can be given is to simply give a brief description of the devices that have been perfected in recent years that make every firm and executive vulnerable to privacy invasion. The following items are not fantasy or fiction. They are not the imaginary creation of an author of super-spy thrillers. They are not being bought by James Bond but rather by John Q. Businessman.

There are presently available on the market cigarette lighters and attache cases that are really combination cameras and transmitters; fountain pens that are microphones, transmitters, or even noise generators designed to jam transmitters; cuff links that are really miniature microphones; brief cases that conceal voice-activated recording equipment; lamps that are actually radio transmitters; probes that pick up voices through walls; thimble-sized telephone line taps with built-in transmitters; microphones disguised as tie-clips, wrist watches, fountain pens; and wireless transmitters small enough to be concealed in a pack of cigarettes.

This listing only scratches the surface of the electronic devices that are generally available today. Most of these items cost under \$200, so they are well within the means of even the smallest company.

Knowing this, it is difficult for many company executives to rest easy when it comes to either their business or personal life, for indeed, there is no place to hide.

-more-

SECTION II

THE MANY MEANINGFUL BUSINESS APPLICATIONS
OF ELECTRONIC LISTENING DEVICES

Many companies are under the mistaken impression that the prime uses for the myriad of electronic listening and recording devices that fall into the industrial security category are illegitimate ones. While undoubtedly many firms and individuals use this type of equipment to obtain the trade secrets of competitors, there are far more sound and legitimate uses for these amazing devices.

The tape recorder hidden in a brief case may provide the industrial spy with a handy piece of apparatus, but it is also an invaluable aid to the market researcher, sales manager, personnel director, management consultants, lecturer, and a host of other business and professional people.

For example, a personnel director travelling the country to recruit engineers for his firm may find a brief case tape recorder a handy way of being able to review his interviews, catch points that he might have overlooked initially, compare interviewee answers to the same questions, etc.

A sales manager may gain a tremendous insight into the capabilities of his salesmen, the effectiveness of their techniques, weak spots, and other valuable sales information by being able to record a typical day's activities.

-more-

Consumer reaction at point-of-purchase can be dramatically captured only through a candid recording of the buyer's positive and negative responses.

The list of sound, meaningful uses to which management can put this new breed of electronic devices is endless. Some firms utilize them as an insurance policy when it comes to executive promotion and placement. All the psychological tests in the world may not give a company as great an insight into the character, temperament and judgement of a key executive as a few moments of truly candid conversation.

Small businessmen, who heretofore might have avoided taking vacations because they did not feel confident enough to leave the affairs entirely in the hands of their employees, now can rest easy. It is possible for them to go away and through a relatively inexpensive internal security system be able to keep a complete check on exactly what occurs in their absence.

A New York State Supreme Court judge has found that a concealed tape recorder can expedite cases tried before him. The judge records all the cases tried before him. Rather than wade through lengthy written transcripts before coming to a decision, he simply plays back the tape and refers to the written text only when necessary. This method has helped speed the judgement day substantially in many cases brought before this leading jurist.

A well-known Manhattan men's clothing shop has increased its sales volume by more than 35% in six months by using a concealed transmitter to ferret out the real reasons customers were not buying particular pieces of apparel and furnishings. One approach the store used was to leave the customer and his wife alone (most men are not brave enough to buy a suit without the approval of their better half) while the salesman went in the back. Concealed in a cuff link box near the shopper was a miniature microphone and transmitter hooked up to a tape recorder in the stock room. The salesman in the rear could listen to the conversation between the man and his wife, thereby gaining an immediate insight into the couple's initial reaction to the merchandise being considered.

If the comments were negative, the salesman knew whether it was price, style, etc., that was holding up the sale and could try to overcome these roadblocks to consummating the purchase. This technique also gave the management information about their sales force, merchandise, pricing, and a host of other important tidbits that helped increase volume.

Undoubtedly, there are uses and applications of electronic listening and recording equipment that are still unthought of. Each day the devices available to business and industry become more specialized and sophisticated.

Insofar as electronic industrial security devices are concerned, the world of tomorrow is here today.

-more-

SECTION III

AN OUNCE OF PREVENTION

Just as there is no total protection against theft of physical possessions, there is no 100% security program that can completely eliminate industrial espionage. However, there are a number of precautions management can take to raise the quality of its company's internal security to the point where the odds are on its side.

The first questions an executive should ask himself is -- "How valuable are the processes, projects, ideas and brainpower of this organization?" A cardinal rule-of-thumb is -- "Don't spend more on defense than the worth of what you're trying to protect."

In most instances, however, security is less expensive than you might think. For example, in these days of advanced business techniques and automation when a single electric office typewriter can cost you \$800, it is interesting to consider that a basic security recording system is available for between \$400 and \$600. Next time you sit down to figure out your office expenditures and where security equipment can fit into the overall picture, perhaps you should bear some of these comparative costs in mind. A small chart we have prepared gives some indication of how little security actually can cost a company.

COST ANALYSIS CHART

1. One clerical person annually costs your company anywhere from \$4,000 to \$6,000.
2. One executive annually draws a salary upwards of \$10,000.
3. One adding machine costs \$250 to \$350.
4. One office copying machine costs \$300 to \$600.
5. Your annual telephone bill is in the thousands of dollars.
6. Automated equipment costs thousands of dollars.
7. A basic security system is \$400 to \$600.

- more -

If you are engaged in a business where your operation is ieterally an open book, you probably have little to worry about. However, if your trade secrets play an important part in your profit picture and your mode of business, you should guard them with the same zealousness that the government applies to classified information. Most businesses with their own classified information to protect would do well to apply military security thinking to their industrial security program.

Some companies make periodic checks of key personnel every six months. Generally these are most effective if the subject doesn't know that this type of security clearance is being conducted. Many times, rather than turn up something that is detrimental to the person under surveillance, quite the contrary occurs.

A small firm recently had its suspicions aroused by a key executive. After employing a number of security approaches, they not only found that he was beyond reproach but a more highly skilled and competent employee than they had realized. These joint discoveries led the company to promptly promote the executive and give him far more authority and responsibility than they would have ever considered doing if their minds had not been put at ease about him.

Another aid to minimizing company leaks is not giving any more information than you have to to any single individual. This again goes back to the military principle about "the need to know". Whoever needs to know

sensitive data gets it. Others get nothing. And an employee's need to know should not depend on his position but on his function.

Just as we were educated during the war to be careful of what we said lest we give vital information to the enemy, companies would be well advised to initiate their own educational security programs. Employees should be made security conscious. Security is not a team but an individual effort.

One major cosmetics firm recently was horrified to find that its employees were inadvertently giving valuable new product information away over the phone to competitors. The competing firms would simply have its people call pretending to be consumers looking for a particular product that did not exist. The conversation would go something like this:

SPY: Could you tell me where I can buy your new moist lipstick?

EMPLOYEE: I'm sorry but I don't believe we have a moist lipstick on the market.

SPY: I'm sure I saw an ad that said your company was coming out with one.

EMPLOYEE: Well, we do have a new series of liquid rouges that we're bringing out in the fall, but I don't think we've announced them yet.

Having been made aware of the situation, the company initiated a program of security education to employees and began monitoring the majority of phone calls going through its switchboard. It quickly put an end to the information leaks as well as uncovering the source of a number of thefts and unauthorized long distance calls.

- more -

The keynote of any educational employee security program should be the old World War II slogan that the enemy is always watching. Employees should be made aware of the kind of information that competitors would like to obtain, such as research and development progress reports, design information, new advertising and marketing approaches, statistical data, and sources of critical supplies.

Other internal security precautions that a firm should consider taking to safeguard its privacy include:

- (1) seeing to it that executive and other personnel clean their desks nightly,
- (2) creating security perimeters around highly sensitive areas,
- (3) locate personnel offices away from strategic areas such as the research and development laboratories,
- (4) protect sensitive areas with hidden TV cameras, microphones, and other detection devices, and
- (5) microfilm important files and keep them in a protected area away from your main office or plant.

All of these steps will help put the odds in your favor when it comes to protecting your privacy; but to obtain even greater protection, a company should consider turning the very electronic devices that might be used against them to their advantage by incorporating them into their security system.

SECTION IV

PROTECTING AGAINST INDUSTRIAL ESPIONAGE

While the age of electronic miracles has made every company and individual a ripe target for hidden microphones, concealed cameras, disguised tape recorders and the rest of the apparatus of the professional snooper, there is no reason that this same knowledge cannot be applied to protecting rather than invading privacy.

Only a few years ago de-bugging was a tremendously expensive and, in many cases, fruitless pursuit. This situation has changed radically.

Recently there has been introduced on the market a number of practical and inexpensive devices that go a long way towards thwarting industrial spies, snoopers, and others who seek to pry. There are "white noise generators" which interfere and thwart any bugging attempt using a transmitter. This noise generator acts as a jamming device and renders any transmitting impossible. However, the oldest "de-bugger" in use is still considered quite efficient: --a loud radio playing music.

Another two items which can help a company feel more securely about its privacy are a transmitter detector and a versatile warning device. The detector is used to locate the frequency of transmission and to determine the location of any transmitter hidden on the premises or concealed on a

- more -

person. It is the unit most often used by investigators for searching houses or offices for "bugging" devices.

The warning device indicates by a blinking light the presence of any transmitter, whether planted or surreptitiously carried by a person. Its small, inconspicuous size and design makes it possible for an executive to keep it atop his desk or over his office door. There also exists a great deal of "de-bugging" equipment costing many thousands of dollars, which is only useful when operated by experienced detection-trained personnel.

The other tools of the industrial spy trade, such as concealed cameras, disguised tape recorders, hidden microphones and a myriad of other specialized electronic equipment, can also be used to safeguard a company's privacy. The best source of information as to what are the best steps for any particular company or individual to take in this respect are, of course, firms that specialize in this field and whose personnel are trained and adept at security techniques.

A professional industrial security firm will know exactly where to look. For example, a major electronics firm was having its new processes pilfered. They checked their offices and conference rooms but could find nothing wrong. They called in some security experts, who started out by looking in the bathroom. Their search was immediately rewarded by finding hidden in the sink a microphone and transmitter that was picking up every word said in the executive men's room.

A major department store also used electronic help to uncover the

culprits in a series of systematic thefts that had cost the company nearly \$250,000.

The store was continuously and unaccountably finding that its appliance department was sustaining significant losses in merchandise. Having narrowed the type of merchandise and department from which it was missing down to this one, the store hired a firm to install professional surveillance equipment both in the stock room and on the sales floor. Phone calls to these departments were monitored. Hidden microphones and tape recorders picked up whatever was said in these two key areas. Within a few weeks it was discovered that two salesmen working with an accomplice were writing fraudulent sales slips, selling merchandise at marked down prices, and in other ways cheating the store of thousands of dollars a week in merchandise.

So bear in mind as you review the true examples cited in these pages that "security equipment", "surveillance equipment", or even the term "spy equipment", refer to devices that have many, many sound, honest, helpful, and legitimate uses. These instruments are becoming standard office equipment and, like the modern computer, can be put to highly effective uses in business today. It is the aim of Zelex Marketing Corporation to help industry find a proper and useful place for security-surveillance equipment.

The End